ubuntu

Ubuntu Livepatch

The Ubuntu Livepatch service lets you apply critical kernel security fixes to your Ubuntu LTS systems without rebooting.

Available to Ubuntu Advantage for Infrastructure customers, the Ubuntu Livepatch Service reduces planned or unplanned downtime while maintaining compliance and security.

About Ubuntu Livepatch

The Ubuntu Livepatch Service delivers live kernel patching to Ubuntu LTS[1] systems eliminating the need to reboot outside a planned maintenance window. Ensuring the security and efficiency of an Ubuntu system has never been easier.

Available to Ubuntu Advantage customers, you can perform patching without interrupting your mission-critical workloads and in-memory databases, saving the cost of downtime and increasing service availability.

UA Infrastructure gives the world's largest enterprises the assurance they need to run mission-critical workloads such as enterprise databases, virtual/cloud hosts or infrastructural services on Ubuntu.

The Ubuntu Livepatch Service is also available for personal use for free up to a maximum of three machines.

Ubuntu Livepatch on-prem

Livepatch on-prem enables full control of patch rollout and allows for easier tracking of the state of registered machines. Livepatch on-prems is available to the cloud of your choice.

Key benefits

Reduce unplanned maintenance

Kernel security updates represent a deeply impactful form of maintenance. Security vulnerabilities mean any delay in patching them increases the risk of exposure. However, kernel updates usually require a reboot, triggering other consequences usually reserved to be addressed in a planned maintenance window. With Ubuntu Livepatch, many security updates will not carry the reboot penalty, which increases predictability in operations.

Maximise service availability

Mission-critical workloads like enterprise databases, virtual/cloud hosts or infrastructure services can't afford downtime. The Ubuntu Livepatch Service applies kernel fixes in microseconds, without restarting your Ubuntu LTS system. Fewer reboots means improved service availability.

Maintain security and compliance

When a security loophole is identified in the Linux kernel, patching is the only way to reduce your exposure from malicious attack. Finding a downtime window to address security vulnerabilities can be challenging, particularly for large-scale and production deployments. The Ubuntu Livepatch Service applies security critical Linux kernel patches without rebooting, keeping your Ubuntu LTS systems secure and compliant.

Control rollout of patches

Livepatch on-prem allows you to define rollout policy and remain in full control of which machines will get updated and when. To keep your machines up-to-date, the on-prem service regularly syncs with Ubuntu Livepatch and obtains the latest patches. Furthermore, the on-prem server allows you to set the policy for staged releases and apply a new patch to a controlled subset of machines across the data center and after validation apply the patch to a wider set of machines in as many stages as needed.

Contain machines within datacenter

Enabling the Livepatch client on machines requires access to the external Ubuntu Livepatch service to fetch the patches. However, with Livepatch on-prem, the machines are contained within the data center as the patches are fetched from the internal service only.

1 Ubuntu 14.04 LTS systems must use the Hardware Enablement kernel.

System requirements

Ubuntu and kernel requirements

Ubuntu Livepatch is available for:

Ubuntu release	Architecture	Kernel Version	Kernel Variants
Ubuntu 20.04 LTS	64-bit x86	5.4 (GA)	generic, lowlatency, aws, azure, oem
Ubuntu 18.04 LTS	64-bit x86	5.4 (HWE)	generic, lowlatency
Ubuntu 18.04 LTS	64-bit x86	4.15 (GA)	generic, lowlatency, aws, oem
Ubuntu 16.04 LTS	64-bit x86	4.15 (HWE)	generic, lowlatency, azure
Ubuntu 16.04 LTS	64-bit x86	4.4 (GA)	generic, lowlatency, aws
Ubuntu 14.04 ESM	64-bit x86	4.4 (HWE)	generic, lowlatency

Ubuntu livepatches work on Ubuntu servers and desktops, on physical machines, virtual machines and in the cloud.

Deployment requirements

Requirements to deploy Ubuntu Livepatch depend on the use case, and can range from storing patches on local storage in one service to proper HA solution with using replicated object storage behind the service for patches.

FAQs

What is Ubuntu Livepatch?

- Ubuntu Livepatch updates your Ubuntu LTS system's kernel with the highest and most critical security vulnerabilities, without requiring a reboot in order to take effect.

Who is entitled to Ubuntu Livepatch?

- Every system covered by an Ubuntu Advantage support contract is entitled to use the Ubuntu Livepatch Service at no additional cost, starting at UA Infrastructure Essential for $75/year for virtual machines or $225/year for physical machines.
- Personal users of Ubuntu can subscribe to up to three machines (laptop, server or cloud) free of charge.

How do I enable Ubuntu Livepatch?

- To enable, run the command:

```
$ sudo ua enable livepatch
```

- You should see output like the following, indicating that the Livepatch snap package has been installed.

```
One moment, checking your subscription first
Installing snapd
Updating package lists
Installing canonical-livepatch snap
Canonical livepatch enabled.
```

- To check the status of Livepatch once it has been installed use this command:

```
$ sudo canonical-livepatch status
```

How can I control the deployment of Livepatches on Premises?

- It is possible to exercise control on the deployment of the livepatches by Canonical and deploy them on your infrastructure with a policy of your choice. Ubuntu Livepatch on-prem can be self-deployed or deployed by Canonical on a cloud of your choice.

How many servers can Livepatch on-prem handle?

- One server with 2 cores and 8GB memory with at least 100 GB of disks can handle thousands of clients; we recommend to adjust according to your number of users and configuration.

How can I use the Livepatch on-prem service if I am an UA Infrastructure customer?

- Use of the on-prem service is included in the price of UA Infrastructure. The service provides a license to download and install a single instance of Livepatch on-prem.

How does this service compare to Oracle Ksplice, RHEL Livepatching and SUSE Livepatching?

- While the concepts are largely the same, the technical implementations and the commercial terms are very different. Ubuntu Livepatch is based on the upstream Linux kernel livepatching technology. Oracle Ksplice is a proprietary solution. RHEL and SUSE currently use their own homegrown kpatch and kgraft implementations, respectively.
  - Oracle Ksplice is available for Oracle Linux and RHEL servers with an Oracle Linux Premier Support license ($2299/node/year)
  - RHEL Livepatching requires a Red Hat Enterprise Linux Server Standard Subscription of $799/node/year
  - SUSE Livepatching is available as an add-on to SUSE Linux Enterprise Server subscription at $2,150/node/year

More on Ubuntu Advantage

Ubuntu Advantage for Infrastructure is the enterprise security maintenance and support package from Canonical. As well as connecting you to the world's leading experts on Ubuntu-based physical, virtual and cloud-based systems, UA Infrastructure customers gain access to Landscape, our award-winning systems management tool.

Landscape lets you run desktop, server and public cloud deployments, or build and manage private OpenStack clouds from a single interface. It is easy to set up, easy to use and requires no special hardware.

It features:

- Management at scale
- Deploy or rollback security updates
- Compliance reports
- Role-based access
- Informative monitoring
- The Ubuntu Livepatch Service

To purchase UA Infrastructure visit ubuntu.com/advantage.

Get started with Livepatch

To get your authorisation code, visit ubuntu.com/advantage.

To purchase Ubuntu Livepatch, including Livepatch on-prem, through the Ubuntu Advantage for Infrastructure subscription, please contact our team below:

(UK) +44 203 656 5291
(US) +1 737 2040291

Or email sales@canonical.com

CANONICAL